KATHLENE W. LOWE (SBN 145404)
KENT J. SCHMIDT (SBN 195969)
JOHN P. CLEVELAND (SBN 239749)
DORSEY & WHITNEY LLP
38 Technology Drive, Suite 100
Irvine, CA 92618-5310
Telephone: (949) 932-3600
Facsimile: (949) 932-3601

Attorneys for Defendant
NEW ALBERTSON'S, INC.

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

RAYMOND W. LONDON, on behalf of Himself and All Others Similarly Situated, Plaintiff, vs. NEW ALBERTSON'S, INC.; CERBERUS CAPITAL MANAGEMENT (CALIFORNIA), LLC; and DOES 1 through 25, inclusive, Defendants.	CASE NO.: 08-1173 HC AB Assigned to: Hon. Marilyn Huff **MEMORANDUM OF POINTS AND AUTHORITIES OF DEFENDANT NEW ALBERTSON'S, INC. IN SUPPORT OF ITS MOTION TO DISMISS** **Hearing:** Date: August 11, 2008 Time: 10:30 a.m. Courtroom: 13, Fifth Floor Complaint filed: May 29, 2008

/ / /

/ / /

/ / /

TABLE OF CONTENTS

INTRODUCTION 1

FACTS 2

ARGUMENT 4

A. Plaintiff Lacks Standing to Sue 4

1. Plaintiff Cannot Assert Third-Party Standing 4

2. Every Plaintiff Must Suffer Injury-In-Fact to Have Standing 5

B. The Complaint Fails to State a Claim for Violation of the CMIA 7

1. Background of the CMIA and its Legislative Intent 7

2. The CMIA's Disclosure Exceptions Permit the Conduct At Issue 9

(a) Section 56.10(c)(16) Expressly Permits Using a Third Party to Encode, Encrypt or "Anonymize" Data to Remove Identifying Information 9

(b) Section 56.10(c)(14) Expressly Permits the Conduct Alleged in the Complaint Because it is Authorized by the Privacy Rule 10

C. Even if the CMIA Were Read to Prohibit the Conduct At Issue, the First Amendment Prevents Its Application to Anonymized Data 11

D. The Complaint Fails to State a Cause of Action for Breach of Contract or the Implied Covenant of Good Faith and Fair Dealing 14

1. Elements of a Breach of Contract 14

2. Albertsons' Privacy Notice Does Not Apply to De-Identified Data 14

3. No Other Alleged Promises Concern De-Identified Data 15

4. Breach of Implied Covenant of Good Faith and Fair Dealing 16

E. The Complaint Fails to State a Cause of Action for "Suppression of Fact" 16

1. Plaintiff Does Not State A Claim for Fraud 16

(a) Plaintiff Does Not and Cannot Allege the Requisite Duty 17

(b) Plaintiff Fails to Plead Fraud With Specificity 18

F. There is No Reasonable Expectation of Privacy Concerning De-Identified Information and the Breach of Privacy Claim Fails to State a Cause of Action 18

1. Plaintiff Has No Legally Protected Privacy Interest in This Data 19

2. Plaintiff Has No Reasonable Expectation of Privacy in the Circumstances 19

3. There Is No Serious Invasion of Privacy At Issue Here 19

G. The Complaint Fails to State a Cause of Action for Unjust Enrichment 20

H. California Law Does Not Recognize a Trespass Claim, Let Alone A "Trespass to Personalty" Claim 21

I. The Complaint Fails to State a Cause of Action for a Violation of California's Unfair Competition Law 22

1. Plaintiff Cannot Allege Loss of Money or Property 22

2. No Allegations of Unlawful Conduct 22

3. No Allegations of Unfair Conduct 23

4. No Allegations of Fraudulent Conduct 23

CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

CASES

Accuimage Diagnostics Corp. v. Terarecon, Inc., 260 F. Supp. 2d 941 (N.D. Cal. 2003) 22

Bank of the West v. Superior Court, 2 Cal. 4th 1254 (1992) 23

Camp v. Jeffer, Mangels, Butler & Marmaro, 35 Cal. App. 4th 620 (1995) 16

Careau & Co. v. Security Pacific Business Credit, Inc., 222 Cal. App. 3d 1371 (1990) 14, 16

Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co., 20 Cal. 4th 163 (1999) 23

Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of New York, 447 U.S. 557 (1980) 13

Colleen M. v. Fertility and Surgical Associates of Thousand Oaks, 132 Cal. App. 4th 1466 (2005) 8

Consumer Advocacy Group, Inc. v. Kintetsu Enterprises of America, 150 Cal. App. 4th 953 (2007) 22

Craig v. Boren, 429 U.S. 190 (1976) 13

Dinosaur Development, Inc. v. White, 216 Cal. App. 3d 1310 (1989) 20, 21

Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995) 6, 7, 20

Gould v. Maryland Sound Industries, Inc., 31 Cal. App. 4th 1137 (1995) 16

Guz v. Bechtel Nat'l, Inc., 24 Cal. 4th 317 (2000) 16

Haskell v. Time, Inc., 857 F. Supp. 1392 (E.D. Cal. 1994) 24

Hill v. National Collegiate Athletic Ass'n (1994) 7 Cal. 4th 1 .... 18, 19, 20, 23

Hsu v. OZ Optics, Ltd.,
211 F.R.D. 615 (N.D. Cal. 2002) 14

Illinois Dept. of Transp. v. Hinson,
122 F.3d 370 (7th Cir. 1997) 5

IMS Health Corp. v. Ayotte,
490 F. Supp. 2d 163 (D.N.H. 2007), *appeal pending* (1st Cir. Case No. 07-1945) .... passim

IMS Health Corp. v. Rowe,
532 F. Supp. 2d 153 (D. Me. 2008), *appeal pending* (1st Cir. Case No. 08-1248) .... passim

In Re Jetblue Airways Corp. Privacy Litigation,
379 F. Supp. 2d 299 (E.D.N.Y. 2005) 6, 14, 15

In re Stac Electronics Securities Litigation,
89 F.3d 1399 (9th Cir. 1996) 18

In re Trans Union Corp. Privacy Litigation,
326 F. Supp. 2d 893 (N.D. Ill. 2004) 6, 7

Khoury v. Maly's of California, Inc.,
14 Cal. App. 4th 612 (1993) 22

Marketing West, Inc. v. Sanyo Fisher (USA) Corp.,
6 Cal. App. 4th 603 (1992) 17

Moore v. Regents of the University of California,
51 Cal. 3d 120 (1990) 6

Pettus v. Cole,
49 Cal. App. 4th 402 (1996) 8

Pioneer Electronics (USA), Inc. v. Superior Court,
40 Cal. 4th 360 (2007) 18, 20

Plevy v. Haggerty,
38 F. Supp. 2d 816 (C.D. Cal. 1998) 4

Shaddox v. Bertani,
110 Cal. App. 4th 1406 (2003) 8, 10

Shibley v. Time, Inc.,
341 N.E.2d 337 (Ohio App. 1975) 6, 20

Shvarts v. Budget Group, Inc.,
81 Cal. App. 4th 1153 (2000) 24

Tarmann v. State Farm Mut. Auto. Ins. Co.,
2 Cal. App. 4th 153 (1991) 18

Thompson v. Home Depot, Inc.,
2007 U.S. Dist. LEXIS 68918 at *8 (S.D. Cal. September 18, 2007) 6, 22

Thompson v. W. States Med. Ctr.,
535 U.S. 357 (2002) 13

Thrifty-Tel, Inc. v Bezenek,
46 Cal. App. 4th 1559 (1996) 21, 22

U.S. News & World Report, Inc. v. Avrahami,
No. 95-1318, 1996 Va. Cir. LEXIS 518, at 5 (Va. Cir. June 13, 1996) 6

Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.,
425 U.S. 748 (1976) 13

Warren v. Fox Family Worldwide, Inc.,
328 F.3d 1136 (9th Cir. 2003) 4

Watson Laboratories, Inc. v. Rhône-Poulenc Rorer, Inc.,
178 F. Supp. 2d 1099 (C.D. Cal. 2001) 23

Yamaha Corp. of America v. State Bd. of Equalization,
19 Cal. 4th 1 (1998) 11

STATUTES

Bus. & Prof. Code §§ 17200 *et seq.* 1, 22, 23

Bus. & Prof. Code § 17204 22

Civil Code § 56.05 7

Civil Code §§ 56.10 *et seq.* .... passim

Civil Code § 56.36 5

Civil Code §§ 1750 *et seq.* 5

Civil Code § 3345 5

N.H. Rev. Stat. Ann. §§ 318:47-f, 318:47-g, and 318-B:12(IV)(2006) 11

OTHER AUTHORITIES

45 C.F.R. § 164.501 11

45 C.F.R. § 164.502 11

67 Fed. Reg. 53182 (Aug. 14, 2002) 11

Fed. R. Civ. Proc. 12(b)(6) 4

1 Witkin, *Summary of California Law (9th ed. 1987),* Contracts 21

1 Witkin, *Summary of California Law (10th ed.),* Contracts 16

15 Moore's Federal Practice (3d ed. 2008) 4, 5

Assembly Bill 262 8

California Const., Article I, Section 1 23

U.S. Const., First Amendment .... passim

INTRODUCTION

In this putative class action, Plaintiff Raymond W. London ("Plaintiff") complains that, after he filled prescriptions at a Sav-On drugstore owned by Defendant New Albertson's, Inc., Albertsons sold "de-identified information" about his prescriptions to "data mining companies" ("DMCs"). "De-identified information" has been stripped of all data which could identify the individual to whom the prescription was issued (name, address, telephone number, email address, social security number). That de-identified data becomes "prescriber-identifiable" after DMCs combine it with information about doctors which they obtain from the American Medical Association and other sources. The resulting aggregated data (from pharmacies and from medical associations) reveals specific details about the prescribing habits of individual physicians. DMCs sell this de-identified aggregated data to pharmaceutical companies, which use that information in targeted marketing campaigns to persuade doctors to prescribe patented medications.[1]

Plaintiff alleges that Defendants' sales of de-identified data violate two California statutes: its Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.10 *et seq.*, and its Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.* Neither law prohibits these data sales, and Plaintiff's statutory claims also fail First Amendment scrutiny. He also asserts six common law causes of action arising from the same conduct: breach of contract and of the implied covenant of good faith and fair dealing, fraud (suppression of fact), breach of privacy, unjust enrichment, and trespass to personalty.

Running through all of Plaintiff's claims are two themes: that these data sales invade his privacy rights, and that he "owns" the de-identified data about his prescriptions. Because neither premise has any basis, his entire complaint must fail. In addition, Plaintiff lacks standing to complain about Defendants' sales of data regarding his physicians' prescribing practices.

---

[1] This data is also "of considerable interest to government agencies, academic institutions, health insurance companies, health maintenance organizations, and other entities" to whom DMCs also sell this data. *IMS Health Corp. v. Rowe*, 532 F. Supp. 2d 153, 158 (D. Maine 2008). *Accord: IMS Health Inc. v. Ayotte,* 490 F. Supp. 2d 163, 166 (D.N.H. 2007). The Complaint speaks only about DMCs' sales to pharmaceutical companies, though, and ignores all these other salutary uses of the same data.

Each of his claims also fails for other, independently sufficient reasons. His CMIA claim fails both because the CMIA does not protect de-identified data and because these data sales are protected by one or more exceptions to the CMIA's prohibition of data use. His contract claim fails because it is premised on a document (Albertsons' Notice of Privacy Rights) which only protects individually identifiable information, not the anonymized data at issue. His implied covenant claims fails because it merely duplicates his contract claim and because the contract claim is itself deficient.

Plaintiff also claims that Albertsons defrauded him by failing to disclose that it would sell his de-identified data. This claim does not allege facts which would create a duty to disclose and it fails to allege fraud with specificity. Plaintiff's common law privacy claim fails because he has no privacy right in information about third parties (doctors) and no reasonable expectation of privacy for de-identified data. His unjust enrichment claim fails because information about his doctors' prescribing practices does not belong to him and because Defendants were not unjustly enriched by the alleged conduct.

Stretching the bounds of artful pleading, Plaintiff next asserts a "trespass to personalty" claim whose premise is that he has a property right in his de-identified information. But since Plaintiff does not in fact own that data and since it is already in the public domain, he has no trespass claim. This claim also fails because there is no authority for the proposition that data—let alone de-identified data—is a property right which could be the subject of a trespass claim.

Finally, Plaintiff includes the obligatory Unfair Competition Law ("UCL") claim—a familiar staple in any consumer class action lawsuit. The UCL theory is of course premised on the notion that the alleged practice is "unfair," "fraudulent" and/or "illegal." Plaintiff has failed to allege facts supporting this or any of his other claims or theories, and he cannot allege that he has lost money or property, an essential element of a *prima facie* claim under the UCL.

Plaintiff has therefore failed to state a claim upon which relief may be granted and this Court should dismiss this action with prejudice because it cannot be cured through amendment.

FACTS

Plaintiff's Complaint contains extensive allegations that have no bearing on whether Plaintiff states a claim against these defendants, and which are instead designed to provoke resentment at pharmaceutical companies. While pharmaceutical companies are a popular target (perhaps second only to oil companies), none is named as a Defendant in this case.[2]

The essence of these interminable allegations is that the pharmaceutical industry uses de-identified prescription information, combined with physician-specific data, to create "prescriber-identifiable data,"[3] which pharmaceutical companies use to market prescription drugs to doctors. There is **no** allegation (and there cannot be one) that Defendants sell individually identifiable information about Plaintiff or any other pharmacy customer to any DMC. Instead, the conduct at issue is Defendants' sale of data to DMCs which, when aggregated, reveals the prescribing practices of individual *doctors* – what drugs they prescribe, in what dosages, what generic substitutes they prescribe, and the like.

The allegations which address Defendants' role in this process are sparse. The process begins when a patient provides his drug prescription to a pharmacy to be filled (Compl. ¶ 7.A). The patient provides not only the information on the prescription, but also his name, address, and telephone number (*id.* ¶ 7.B). DMCs buy Albertsons' prescription data (*id.* ¶ 8). They acquire that data by installing software on Albertsons' mainframe computer which captures and collates data about all prescriptions (*id.* ¶ 12). *There are no other fact allegations about any conduct by any Defendant; all remaining fact allegations relate only to conduct by the non-party DMCs and pharmaceutical companies.* The DMCs remove all information which could identify individual patients before transferring any data to their pharmaceutical company customers (*id.* ¶ 9).[4] A number is assigned to each de-identified patient which permits prescription information to be correlated for each patient but "purportedly" does not allow the patient's identity to be determined (*id.* ¶ 12). Before DMCs sell this data, they combine it with other information about the doctor who issued each prescription (*id.*). That data, obtained from the AMA and other third parties, identifies the prescriber's correct name, address, specialty, and other professional information (*id.* ¶ 13).

---

[2] Defendant Albertsons owns supermarkets and pharmacies in many states. Defendant Cerberus is merely the partial owner of a company which purchased some Albertsons stores in 2006 and is therefore not even a proper defendant. Plaintiff also recently filed a Doe amendment which brought in SaveMart as a new defendant. SaveMart purchased some Northern California supermarkets from a third party in 2007.

[3] See, *e.g.*, Compl. ¶¶ 13, 14, 16, and 18 for references to "prescriber-identifiable data."

[4] This allegation is incorrect. All information which could identify an individual patient is removed at Albertsons' server *before* it is transmitted to DMCs or any other third party. However, for purposes of this motion only, Albertsons treats this allegation as true.

ARGUMENT

A court should grant a motion to dismiss where it appears from the allegations of the complaint that "plaintiff can prove no set of facts in support of his claim which would entitle him to relief." *Plevy v. Haggerty*, 38 F. Supp. 2d 816, 820 (C.D. Cal. 1998). While under Rule 12(b)(6) a court must assume all factual allegations are true, it is not required to credit Plaintiff's conclusory legal allegations. *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003)("[A court does] not . . . necessarily assume the truth of legal conclusions merely because they are cast in the form of factual allegations"). Applying this standard to Plaintiff's Complaint, no viable cause of action is stated and the Court should therefore grant this motion to dismiss.

A. Plaintiff Lacks Standing to Sue

1. Plaintiff Cannot Assert Third-Party Standing

"The well established rule of third-party standing is that in the ordinary course, a litigant must assert his or her own legal rights and interests, and cannot rest a claim to relief on the legal rights or interests of third parties." 15 Moore's Federal Practice (3d ed. 2008), § 101.51[3][a]. This requirement assures that federal courts refrain from deciding abstract issues of public importance, prevents them from adjudicating rights whose holders may not wish to assert them, and recognizes that the holders of rights are likely to be the most effective advocates. *Id.* at 101-88.6 – 101:90. To establish such standing, the third party must be unable to protect its own interest. *Id.*, § 101.51[3][c][iii] at 101-94.

Plaintiff is in fact a third party to the interests at issue, since it is information about his doctors, not information which can be linked to him individually, which Defendants sell to DMCs. That is, according to the Complaint, the data which DMCs sell has value to pharmaceutical companies only because it aggregates the prescription histories of many anonymous patients to reveal the prescribing practices of individual doctors. Information about any particular individual has no value to those companies, not merely because it is anonymous, but instead because it cannot help identify any doctor's overall prescribing habits. Only when all the prescription data generated by one doctor to one patient is later aggregated with prescription data generated by the same doctor for other patients and filled at the same or other pharmacies will the doctor's overall practices be revealed. If anyone has first party standing to complain about these data sales to pharmaceutical companies, then, it is the physicians whose prescribing practices are revealed by that data and who are then targeted in individually tailored marketing pitches.

Stated differently, the data is not "about" Plaintiff, because no one could discern from reviewing that data that any individual prescription was issued to him rather than to some other individual. Plaintiff therefore cannot realistically contend that it was "his" data which Albertsons has sold. He is a third party to the interests being asserted, and he cannot seriously claim that physicians are unable to protect their own interests. He cannot assert third party standing.

2. Every Plaintiff Must Suffer Injury-In-Fact to Have Standing

In order to establish standing, every plaintiff must not only vindicate his own rights, but must also suffer injury-in-fact. *Id.*, § 101.40[1] at 101-32 (first party standing), and at § 101.51[3][c][i] at 101-90 (third party standing). Among other things, this requirement prevents "'cause' mongers from wresting control of litigation from the people directly affected." *Illinois Dept. of Transp. v. Hinson*, 122 F.3d 370, 373 (7th Cir. 1997).

Plaintiff does not and cannot allege the requisite injury in fact. His complaint contains only general and conclusory allegations that he and the class have been harmed or damaged, except for one allegation that their damages consist of the profits Defendants received from data sales. *Compare* Compl. ¶¶ 26 at 12:16-17 and 39 at 16:27-28 (general allegations of damage) *with* ¶ 54 at 21:14-18 (class deprived of the profits Defendants have received). His only other damages claims appear in his Prayer for Relief which, oddly, seeks compensatory damages "as permitted by the CLRA"[5] even though he pleads no cause of action under that statute; treble damages under Civil Code Section 3345 (also odd, since it applies only to claims by senior citizens and disabled persons); disgorgement of profits; and compensatory and statutory damages under the CMIA (i.e., $1,000 per violation).[6] Prayer,

---

5 The CLRA is the California Consumer Legal Remedies Act, Cal. Civil Code §§ 1750 *et seq.*

6 That statutory penalty appears in Civil Code § 56.36(b)(1).

Compl. at 27:19-28:8. The question, though, is what cognizable harm Plaintiff (or the class) could have sustained by virtue of the sale of data regarding third parties (doctors). Unless Plaintiff and the class have some protectible property right in the data at issue, they do not have any injury-in-fact.

Plaintiff cannot assert that he has lost "property" by virtue of Defendants' sale of prescription data. First, Defendants are selling data which cannot be linked to Plaintiff or any other class member. Second, although his Complaint characterizes Plaintiff's medical information as his "property" (Compl. ¶¶ 7.B at 3:17, 7.C at 3:24-26), the few cases which have considered similar questions have refused to recognize a property right in personal information. *Thompson v. Home Depot, Inc.*, 2007 U.S. Dist. LEXIS 68918 at *8 (S.D. Cal. September 18, 2007)(Gonzalez, C.J.)(rejecting plaintiff's claim that his personal information, used by defendant for marketing purposes, is "property"), *citing In Re Jetblue Airways Corp. Privacy Litigation,* 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005)("There is . . . no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large"), and *Dwyer v. American Express Co.*, 652 N.E.2d 1351, 1356 (Ill. App. 1995)(individual names have "little or no intrinsic value to . . . a merchant"). *Accord: In re Trans Union Corp. Privacy Litigation,* 326 F. Supp. 2d 893, 902-03 (N.D. Ill. 2004)(individual plaintiffs' names have no intrinsic value); *Shibley v. Time, Inc.*, 341 N.E.2d 337, 340 (Ohio App. 1975); *U.S. News & World Report, Inc. v. Avrahami,* No. 95-1318, 1996 Va. Cir. LEXIS 518, at 5 (Va. Cir. June 13, 1996). And *see Moore v. Regents of the University of California,* 51 Cal. 3d 120, 136-39 (1990)(denying plaintiff property rights in his body and his biological information).

In re Jetblue, supra, is also noteworthy because there, as here, plaintiffs asserted that they provided their personal information to JetBlue only for the specific purpose of buying an airplane ticket, and that they did so on

> the promise that their personal information would be safeguarded consistent with the terms of [JetBlue's] privacy policy. They had no reason to expect that they would be compensated for the 'value' of their personal information. In addition, there is absolutely no support for the proposition that the personal information of a JetBlue passenger had any value for which that passenger could have expected to be compensated. [379 F. Supp. 2d 299, 327.]

This case is also analogous to *Dwyer* and *In re Trans Union, supra,* both of which involved defendants' sales of data about individual customers which was used to create target marketing lists.

Dwyer, 652 N.E.2d at 1353; *Trans Union,* 326 F. Supp. 2d at 895. In both cases, plaintiffs asserted privacy claims (among others). In both cases, the courts held that a single customer's name has little or no intrinsic value to the purchasers of such lists, and that value is instead created only when the defendant categorizes and aggregates those names. *Dwyer,* 652 N.E.2d at 1356; *Trans Union,* 326 F. Supp. 2d at 902. The alleged property right asserted by this Plaintiff is even more attenuated, since no one could identify any particular prescription as having been issued to him – unlike the plaintiffs in *Dwyer* and *Trans Union,* whose personal information had in fact been disclosed to third parties.

Plaintiff cannot establish either first or third party standing because he has suffered no injury-in-fact. His entire Complaint should therefore be dismissed with prejudice.

B. The Complaint Fails to State a Claim for Violation of the CMIA

1. Background of the CMIA and its Legislative Intent

Subject to certain exceptions, the CMIA prohibits the use or disclosure of "medical information" without a patient's prior authorization. Civil Code §§ 56.10(a) and (d). "Medical information" is defined as "individually identifiable information." Civil Code § 56.05(g). "Individually identifiable information" is information which

> includes or contains any element of **personal identifying information** sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, **reveals the individual's identity**.

Civil Code § 56.05(g) (emphasis added). Because the statute reaches only such "individually identifiable information," Plaintiff cannot establish a CMIA violation. Once medical data is de-identified, the information is what the CMIA calls "anonymiz[ed] data"—information that does not disclose "individually identifiable information." Cal. Civ. Code § 56.10(c)(16). The CMIA simply does not govern the handling of de-identified data because, by definition, that data is not "individually identifiable information."

This conclusion is supported not only by the plain language of the statute, discussed above, but also by its legislative history and case law. In 2003, the Legislature considered and debated amendments to the CMIA which added a proscription against the use of individually identifiable information for marketing (Civil Code Section 56.10(d)). These changes initially appeared in

Assembly Bill 262 ("AB 262"). AB 262 contained two elements: (1) the marketing prohibition which eventually became part of Section 56.10(d), and (2) a proposed "Do Not Use" list, which would have protected participating physicians from sale of the same data at issue in this case. The first element of AB 262 was enacted in 2004, but the second element – the proposed "Do Not Use" list – was not enacted into law.[7] The proposal was that, if doctors placed their names on the "Do Not Use" list, pharmacies could not sell prescribing information about them to any third party.

The "Do Not Use" portion of AB 262 died in Conference.[8] The Senate Committee on Business and Professions considered this proposed legislation and concluded that the "Do Not Use" provisions did not belong in the CMIA:

> **It seems clear that the CMIA was intended to apply to patient medical information and not physician prescription information** which may or may not be made available to other persons or entities depending on the specified restrictions within [the "Do Not Use" portion of AB 262].

Lowe Decl. ¶ 5 and Exh. B. This legislative history confirms that the CMIA was never intended to govern the use or transfer of information which is not individually identifiable. Plaintiff cannot seriously contend that the CMIA prohibits the transfer of de-identified data since the California Legislature chose not to adopt legislation prohibiting this very practice.

Finally, these conclusions are further corroborated by case law. Every California case interpreting and applying the CMIA has, without exception, involved the transmission of *identifiable* information to a third party, allegedly without consent. For example, in *Colleen M. v. Fertility and Surgical Associates of Thousand Oaks*, 132 Cal. App. 4th 1466 (2005), a fertility clinic disclosed a patient's medical history to her ex-fiancé in response to a subpoena; her medical and identifying information was disclosed. In *Shaddox v. Bertani*, 110 Cal. App. 4th 1406 (2003), a dentist disclosed to a police department his suspicions that a police officer was addicted to prescription pain medicine; his medical and identifying information was disclosed. *Pettus v. Cole*, 49 Cal. App. 4th 402 (1996), challenged an employer's use of psychiatric information about an employee to force him into an

---

7 Lowe Decl. ¶¶ 2-7 and Exhs. A-D.

8 *Id.*, Exh. A.

inpatient alcohol treatment program and ultimately to terminate his employment; his medical and identifying information was disclosed.

These cases involve the type of communications the CMIA was intended to address. Not one reported case has involved de-identified information. Plaintiff's attempt to stretch the statute beyond its intended application is unavailing as the CMIA was simply not intended to address the conduct alleged in the Complaint. Thus, even accepting all allegations as true, the CMIA claim fails as a matter of law.

2. The CMIA's Disclosure Exceptions Permit the Conduct At Issue

As discussed above, the statute contains two prohibitions: disclosure (Section 56.10(a)) and use (Section 56.10(d)). Both of those prohibitions are subject to twenty-seven separate exceptions (or "safe harbors"). Cal. Civ. Code § 56.10(b) and (c). Conduct that would otherwise be prohibited is permitted if one of the exceptions applies. Even if this Court were to conclude, notwithstanding the foregoing argument, that the CMIA extends to de-identified data, the conduct at issue falls within at least two of these exceptions. Section 56.10(c)(14) permits disclosures that are "otherwise specifically authorized by law," and Section 56.10(c)(16) allows the transfer of "anonymized" data. Both exceptions are discussed below.

(a) Section 56.10(c)(16) Expressly Permits Using a Third Party to Encode, Encrypt or "Anonymize" Data to Remove Identifying Information

Section 56.10(c)(16) provides:

> The information may be disclosed to a third party for purposes of encoding, encrypting, or otherwise anonymizing data. However, no information so disclosed shall be further disclosed by the recipient in any way that would violate this part, including the unauthorized manipulation of coded or encrypted medical information that reveals individually identifiable medical information.

Cal. Civ. Code § 56.10(c)(16). Two things are apparent from Subdivision (c)(16). First, the plain text of this exception reveals that is permissible to allow a third party to receive data in order to "anonymize" it—or, in the words of the Complaint, "have the information identifying individual patients removed" (Compl. ¶ 9). Second, any further disclosure—*i.e.*, a disclosure beyond that to the party anonymizing the data—must be done in such a way that it does not reveal individually identifiable information.

This exception further confirms that the CMIA does not proscribe the transfer of anonymized or "de-identified" data. Simply stated, even if the conduct alleged in the Complaint falls within the scope of the CMIA's two prohibitions against use and disclosure (and it does not), Subdivision (c)(16) confirms that the conduct falls within an exception and thus does not violate the law. The CMIA claim therefore fails as a matter of law.

(b) Section 56.10(c)(14) Expressly Permits the Conduct Alleged in the Complaint Because it is Authorized by the Privacy Rule

Subdivision (c)(14) allows any disclosure which is otherwise specifically authorized by law. That subsection states:

> The information may be disclosed when the disclosure is otherwise specifically authorized by law, including, but not limited to, the voluntary reporting, either directly or indirectly, to the federal Food and Drug Administration of adverse events related to drug products or medical device problems.

Cal. Civ. Code § 56.10(c)(14). This exception expresses the California Legislature's intent that the CMIA be applied in harmony with other state and federal regulations by providing an important safe harbor to its general prohibition on disclosures of medical information. "Subdivision (c)(14) thus serves as the residuary clause in Section 56.10. It legitimizes a myriad of situations the Legislature may not have cared to spell out, by establishing the principle of permissive disclosure when specifically authorized by law." *Shaddox v. Bertani*, 110 Cal. App. 4th 1406, 1414 (2003).

The question presented in applying Subdivision (c)(14) is quite simply: *does some other state or federal regulation specifically authorize the disclosure at issue?* In *Shaddox,* the only case that has interpreted and applied Subdivision (c)(14), one of the "other laws" which authorized a disclosure was the San Francisco City Charter. The text of this subdivision and of *Shaddox* confirm that the "other law" need not be in the CMIA or even another California statute or regulation.

In this case, the conduct alleged is specifically authorized by the HIPAA[9] "Privacy Rule"

---

9 "HIPAA" is the federal Health Insurance Portability and Accountability Act.

promulgated by the Department of Health and Human Services ("HHS").[10] Any entity to which HIPAA applies (including Defendants) may create information that is not individually identifiable health information by using "protected health information"[11] to create de-identified health information. The information is no longer "protected health information" after it is de-identified. 45 C.F.R. § 164.502(d). Unless protected health information has been so de-identified, its use and disclosure is restricted in much the same manner as that data is restricted under the CMIA. See 45 C.F.R. § 164.502(a).

Because Subdivision (c)(14) allows disclosures "otherwise specifically authorized by law," including federal law, the sale of de-identified data alleged in the Complaint falls within the safe harbor of subdivision (c)(14). Therefore, even if the CMIA were deemed to apply to this conduct, the Complaint fails to state a violation of the statute.

C. Even if the CMIA Were Read to Prohibit the Conduct At Issue, the First Amendment Prevents Its Application to Anonymized Data.

Maine and New Hampshire attempted to regulate the sale of de-identified data. Both states' statutes failed to withstand First Amendment challenge. Accordingly, even if this Court were to conclude that, notwithstanding the foregoing, the CMIA prohibits the sale of de-identified data, this Court should reach the same result as the two courts that have thoughtfully addressed these constitutional challenges.

In *IMS Health Corp. v. Ayotte*, 490 F. Supp. 2d 163 (D.N.H. 2007), *appeal pending* (1st Cir. Case No. 07-1945), IMS challenged New Hampshire's Prescription Information Law[12] based on the First Amendment's guarantee of free speech. That statute barred pharmacies and other entities from transferring or using prescriber-identifiable data for certain commercial purposes. The federal court

---

10 HHS adopted the Privacy Rule pursuant to its "substantive lawmaking" authority granted by Congress and, as such, under California law the Privacy Rule is a "quasi-legislative rule" which has "the dignity of statutes." (RJN Ex. 2 at p. 53182, I(A) Para. 2 [67 Fed. Reg. 53182 (Aug. 14, 2002), codified at 45 C.F.R. pts. 160, 164]) *See Yamaha Corp. of America v. State Bd. of Equalization*, 19 Cal. 4th 1, 10, 11 (1998) (distinguishing substantive lawmaking from interpretative acts and observing that the former has "the dignity of statutes").

11 "Protected health information" is the HIPAA equivalent of the CMIA's "individually identifiable information." It is so defined at 45 C.F.R. § 164.501.

12 N.H. Rev. Stat. Ann. §§ 318:47-f, 318:47-g, and 318-B:12(IV)(2006).

agreed with IMS that the statute unduly restrained commercial speech, and therefore issued a permanent injunction against enforcement of the law.[13]

More recently, the Maine federal district court relied heavily on *Ayotte* to conclude that Maine's similar law was likewise unenforceable because of the First Amendment. *IMS Health Corp. v. Rowe*, 532 F. Supp. 2d 153 (D. Me. 2008), *appeal pending* (1st Cir. Case No. 08-1248). Because the Maine decision follows the logic of *Ayotte*, only the *Ayotte* decision is addressed here.[14]

Both *Rowe* and *Ayotte* addressed the practices of the same DMCs whose business conduct is the subject of the Complaint in this case – IMS, Verispan, and others (Compl. ¶¶ 11, 12).

Following a detailed and instructive explanation about data mining and its use by pharmaceutical companies (490 F. Supp. 2d at 165-170), *Ayotte* concluded that the statute regulated commercial speech. 490 F. Supp. 2d at 175. The court explained that the data at issue *is* "speech" because "the challenged law restricts the transmission of truthful information concerning the prescribing practices of New Hampshire's health care providers. It is not exempt from First Amendment review merely because it targets factual information rather than viewpoints, beliefs, emotions, or other types of expression." *Id.*

Like the CMIA, the New Hampshire law prohibited both the "use" and the "disclosure" of prescriber-identifiable data. The court concluded that the law was a speech restriction because it limited "both the use and disclosure of prescriber-identifiable data for commercial purposes." *Id.* It also reasoned that even a restriction on use (rather than disclosure) would restrain speech because it would prevent pharmaceutical companies "from using prescriber-identifiable information both to identify a specific audience for their marketing efforts and to refine their marketing messages. Such laws are subject to First Amendment scrutiny because they affect both the speaker's ability to communicate with his intended audience and the audience's right to receive information." *Id.*

---

13 Ironically, many passages in that lengthy decision appear almost verbatim in the Complaint filed in this action. The irony arises from the fact that Plaintiff would choose to plagiarize from a decision which establishes that his statutory claims do not survive First Amendment scrutiny.

14 Both cases are currently on appeal to the First Circuit, which heard oral argument in January 2008. *Rowe* is stayed pending that court's decision in *Ayotte* (1st Cir. Case No. 07-1945).

Because the court concluded that the data at issue was commercial speech rather than "pure" speech, it analyzed the constitutionality of the statute under the intermediate scrutiny standard established in *Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of New York*, 447 U.S. 557, 564 (1980). *Id.* at 177. Under that standard, commercial speech restrictions are enforceable only if they support a substantial governmental interest, directly advance the interest asserted, and are not more extensive than necessary to serve that interest. The party seeking to uphold a commercial speech restriction has the burden of proof as to all three elements.

The state Attorney General argued that the law was narrowly drawn and directly advanced the state's substantial interests in protecting prescriber privacy, promoting public health, and containing health care costs. IMS took issue with all three contentions and also argued that the law was invalid even if it was effective because its purposes could be achieved as well or better through alternatives that do not restrict protected speech. *Id.* The court agreed with all of IMS' contentions. In addition, it referred to a Supreme Court comment that "[w]e have previously rejected the notion that the Government has an interest in preventing the dissemination of truthful commercial information in order to prevent members of the public from making bad decisions with the information." *Id.* at 181, *quoting Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 374 (2002).

Albertsons may properly invoke the free speech rights of DMCs and pharmaceutical companies in response to this challenge to pharmacy data sales. The Supreme Court has broadened its general rules on standing in First Amendment cases to allow vendors who have suffered their own injuries to assert the rights of their customers. *See Craig v. Boren,* 429 U.S. 190, 194-95 (1976). Here, the injury Albertsons will suffer if data sales are prohibited will be (1) its own lost revenue from those sales and (2) any statutory penalties or other damages awarded to Plaintiff and the class. In a parallel situation, *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748, 756 (1976), the Court held that consumers of prescription drugs have standing to challenge state restrictions on drug price advertising by licensed retail pharmacists. The Court reasoned that "where a [willing] speaker exists . . . the protection afforded is to the communication, to its source and to its recipients both." Here, Albertsons is a source of the information used by DMCs and pharmaceutical companies and it should therefore also be able to invoke the protection of the First Amendment.

In sum, as noted above, the CMIA does not apply to the de-identified data here at issue. But even if this Court were to conclude otherwise, it should follow the lead of *Ayotte* and *Rowe* and conclude that the First Amendment precludes application of the CMIA to this form of speech.

D. The Complaint Fails to State a Cause of Action for Breach of Contract or the Implied Covenant of Good Faith and Fair Dealing

1. Elements of a Breach of Contract

"A cause of action for damages for breach of contract is comprised of the following elements: (1) the contract, (2) the plaintiff's performance or excuse of nonperformance, (3) the defendant's breach, and (4) the resulting damages to the plaintiff." *Hsu v. OZ Optics, Ltd.*, 211 F.R.D. 615, 619 (N.D. Cal. 2002); *Careau & Co. v. Security Pacific Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1388 (1990). The Complaint fails to satisfy even these elementary requirements.

2. Albertsons' Privacy Notice Does Not Apply to De-Identified Data.

In his general allegations, Plaintiff quotes portions of Albertsons' Notice of Privacy Practices ("Privacy Notice") at Paragraph 30 of his Complaint (at 13:15-14:21). Even though his quotes are misleadingly selective, they still make it undeniably clear that Albertsons' promises are only to protect "Protected Health Information," *not* anonymized information. The Privacy Notice explains that "[w]e are required by federal law to maintain the privacy of health information *that identifies you or that could be used to identify you (known as 'Protected Health Information')*" (*id.* at 13:21-23; emphasis supplied). Throughout the excerpts quoted by Plaintiff are fourteen separate references to "Protected Health Information" – the only type of information which is mentioned in the Privacy Notice. The Notice says nothing whatsoever about the use or disclosure of de-identified information.

In Plaintiff's second cause of action for breach of contract, he quotes again from the Privacy Notice (¶ 47, at 19:6-18) to argue that the Notice creates a contract with him – but again, all references in the quoted text are solely to Protected Health Information. Therefore, Plaintiff's breach of contract claim based on the Privacy Notice fails because the Notice does not apply to the sale of anonymized data.

3. **No Other Alleged Promises Concern De-Identified Data.**

In addition to the Privacy Notice, Plaintiff relies on other alleged express or implied promises by Albertsons as the basis for his contract claim, including promises that "Albertsons would not use Plaintiff and the Class members' *confidential* medical information for the marketing of drugs," that those individuals' "*individually identifiable* medical information would not be shared, sold, used for marketing, or otherwise used or disclosed;" and the like (*id.* ¶¶ 48, 53). Again, however, none of these alleged promises relate to the use or disclosure of *anonymous* pharmacy data. Plaintiff therefore fails to identify any unilateral promise by Albertsons which was allegedly breached. It also strains credulity to suggest that Albertsons made any promise to *Plaintiff* that it would not sell data about *third parties* (doctors) to others.

Plaintiff's own Complaint makes it clear that all personally identifying information is removed before any data is sold to pharmaceutical companies (see, *e.g.,* Paragraphs 9, 12). A more accurate and clearer explanation about the anonymity of this data appears in *Rowe* (532 F. Supp. 2d 153, 162), describing how the data is anonymized at the pharmacy's server even before it is transmitted to the same DMCs whose practices are condemned in Plaintiff's Complaint: "The information to the [DMCs] is encrypted and the [DMCs] are unable to identify a specific patient. There is no real claim that the [DMCs] have violated an individual patient's right of privacy." The court also explained that

> personal patient information has been and will continue to be encrypted and there is no evidence that the current practices of the [DMCs] and the pharmaceutical companies have had or realistically could have any effect on patient confidentiality. . . . [G]iven the encrypted nature of the patient identifiers and the limited remaining information, such a possibility is extremely farfetched, would involve extraordinary efforts on the part of the [DMC] or pharmaceutical company, and would likely violate a host of federal and state laws. There is no evidence that such an attempt has ever been made and the Court views this contention as purely theoretical. [532 F. Supp. 2d at 173 & n.28.]

Similarly, *Ayotte* recognized that, "to comply with state and federal laws protecting patient privacy, participating pharmacies allow plaintiffs to install software on their computer that encrypts any information identifying patients *before* it is transferred to plaintiffs' [i.e., DMCs'] computers" (emphasis supplied). This process "does not allow the patient's identity to be determined." 490 F. Supp. 2d 163, 166.

4. Breach of Implied Covenant of Good Faith and Fair Dealing

Like many jurisdictions, California recognizes that every contract contains an implied covenant of good faith and fair dealing, obligating the contracting parties to refrain from doing anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract. 1 Witkin, *Summary of California Law (10th ed.),* Contracts § 798, at 892.

But this claim must be founded on a contract. *See Gould v. Maryland Sound Industries, Inc.*, 31 Cal. App. 4th 1137, 1153 (1995); *Camp v. Jeffer, Mangels, Butler & Marmaro*, 35 Cal. App. 4th 620, 631 (1995). Because Plaintiff has failed to adequately plead the existence of an enforceable contract, as a matter of law, Plaintiff also cannot establish a claim for breach of the implied covenant of good faith and fair dealing.

Alternatively, if an enforceable contract is pled, the breach of implied covenant claim is duplicative of the contract claim. It is well settled that, where a plaintiff alleges a contract claim and a covenant claim, both based on the same facts and seeking the same damages, the covenant claim is superfluous and should be dismissed. *Guz v. Bechtel Nat'l, Inc.*, 24 Cal. 4th 317, 327 (2000) (breach of implied covenant claim duplicative of contract claim properly dismissed as superfluous); *Careau & Co. v. Security Pac. Bus. Credit*, 222 Cal. App. 3d 1371, 1395 (1990) ("If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded and superfluous as no additional claim is actually stated").

E. The Complaint Fails to State a Cause of Action for "Suppression of Fact"

1. Plaintiff Does Not State A Claim for Fraud

Plaintiff's fourth cause of action is styled "suppression of fact." Assuming that this is a misnamed claim for fraudulent concealment, the threshold question is whether the elements of that cause of action have been pled. The elements of an action for fraud based on concealment are: (1) the defendant must have concealed or suppressed a material fact, (2) the defendant must have been under a duty to disclose the fact to the plaintiff, (3) the defendant must have intentionally concealed or suppressed the fact with the intent to defraud the plaintiff, (4) the plaintiff must have been unaware of the fact and would not have acted as he did if he had known of the concealed or suppressed fact, and

(5) as a result of the concealment or suppression of the fact, the plaintiff must have sustained damage. *Marketing West, Inc. v. Sanyo Fisher (USA) Corp.*, 6 Cal. App. 4th 603, 612-13 (1992).

(a) Plaintiff Does Not and Cannot Allege the Requisite Duty

Plaintiff vaguely alleges that he had a special relationship with his pharmacy in order to allege a prima facie claim of fraudulent omission (Compl. ¶ 63), but this purely conclusory statement must be disregarded on this motion. It should instead be intuitively obvious that the data being sold is not the subject of any special duty, even if we assume *arguendo* that Plaintiff has a fiduciary relationship with his pharmacist.[15] That is, no one is selling any information which can be traced to *Plaintiff* (his name, contact information, or other individually identifying information). Instead, what is being sold is data about his doctors: what they are prescribing and with what frequency. In other words, what is sold is *professional* information (about doctors' prescribing practices), not *personal* information (about Plaintiff). How can the sale of data about third parties breach a duty to Plaintiff?

Ayotte recognized that information privacy laws "protect the privacy of personal information," not the professional information contained in the data at issue. *Ayotte,* 490 F. Supp. 2d at 179 n.13. The court also recognized that "health care providers cannot credibly claim that they have a reasonable expectation that their prescribing practices will remain private because prescriber-identifiable data is routinely disclosed to patients, pharmacies, insurance companies, medical review committees, and government agencies. In other words, because health care providers work in a 'closely-regulated' industry, they have at best a diminished expectation of privacy with respect to their prescribing practices." *Id.* (citations omitted). *Rowe* reached the same conclusion. 532 F. Supp. 2d at 164-65 ("[T]o claim a general right to ownership in prescribing patterns is to assert a novel legal protection to information that is widely available at no charge to countless third parties"), and at 170 ("prescribers cannot prevent a host of entities from reviewing their prescribing patterns").

If such professional information is routinely and properly disclosed to "countless third parties," then it must follow that there is no duty to Plaintiff to disclose the future transfer of professional data about his physicians. Likewise, if doctors are routinely disclosing this data to third parties, it is nonsensical for Plaintiff to claim that his pharmacy must tell him about such data sales, but his doctor need not do so. Plaintiff cannot establish a duty to disclose these data sales to him.

---

[15] There is no California appellate decision which holds that the pharmacist-patient relationship gives rise to a fiduciary duty.

(b) Plaintiff Fails to Plead Fraud With Specificity

When alleging fraud against a corporation, as here, the particularity requirement is stringent. As the court explained in *Tarmann v. State Farm Mut. Auto. Ins. Co.*, 2 Cal. App. 4th 153, 157 (1991), "[t]he requirement of specificity in a fraud action against a corporation requires the plaintiff to allege the names of the persons who made the allegedly fraudulent representations, their authority to speak, to whom they spoke, what they said or wrote, and when it was said or written." *Id.* at 157; *see also In re Stac Electronics Securities Litigation*, 89 F.3d 1399, 1410 (9th Cir. 1996) (complaint fails to sufficiently plead fraud because "it provides no specific facts—no names, no meetings, no internal memoranda or documents, no specific conduct or statement—in support of its theory"). Plaintiff's fraud claim fails to satisfy these and other pleading rules and should be dismissed.

F. There is No Reasonable Expectation of Privacy Concerning De-Identified Information and the Breach of Privacy Claim Fails to State a Cause of Action

In his fifth cause of action for breach of privacy, Plaintiff alleges that he had a legally protected privacy interest "as directed by our Supreme Court in *Hill v. National Collegiate Athletic Ass'n* (1994) 7 Cal. 4th 1" (Compl. ¶ 68). This is of course a legal conclusion which this Court need not accept as true. *Hill* identifies two types of privacy interests—autonomy privacy (i.e., "interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference") and informational privacy (*i.e.*, "interests in precluding the dissemination or misuse of sensitive and confidential information"). *Hill*, 7 Cal.4th at 35. Plaintiff's theory here is apparently informational privacy, which requires him to show: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy. *Id.* at 37. "'If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion of privacy may be adjudicated as a matter of law." *Pioneer Electronics (USA), Inc. v. Superior Court*, 40 Cal. 4th 360, 370 (2007). Based on the facts alleged by Plaintiff, he cannot establish any of the three elements of a privacy claim.

1. Plaintiff Has No Legally Protected Privacy Interest in This Data

The state Attorneys General who defended *Ayotte* and *Rowe* did not even argue that prohibition of de-identified data sales would infringe on *patients'* privacy. *See, e.g., Ayotte,* 490 F. Supp. 2d at 179 ("the Attorney General . . . does not claim that the [prescriber-identifiable data] is used to intrude upon the doctor-patient relationship"). Instead, they argued that the states had a substantial interest in protecting *prescriber* privacy by "limiting unwarranted intrusions into the decision-making process of prescribing physicians" (*id.* at 178). *Ayotte* commented, citing numerous federal cases, that it would "require a substantial extension of existing precedent" to support any argument that the statute protected information privacy – the very claim at issue here. *Id.* at 179 n.13.

As discussed above, information about Plaintiff's individual prescriptions cannot be linked to him. While his anonymized prescriptions do form part of a massive database, no one could tell whether any such prescription was issued to him as opposed to any other pharmacy customer in California. That data is therefore no more "private" than the information captured by the scanner at his local supermarket which records all products he purchases on a given day, and which likewise cannot be tied to him. When he buys a movie ticket, the theatre is probably logging the total number of customers who patronized the same showing of the same movie, but this gives him no privacy right in the data regarding attendance at that show.

2. Plaintiff Has No Reasonable Expectation of Privacy in the Circumstances

"Even when a legally cognizable privacy interest is present, other factors may affect a person's reasonable expectation of privacy." *Hill*, 7 Cal. 4th at 36. "[C]ustoms and physical settings of certain activities may impact an individual's reasonable expectation of privacy." *Id.* Since the data at issue is the same data which was at issue in *Rowe* and *Ayotte*, and since both courts (and both state Attorneys General) recognized that this data is "widely available at no charge to countless third parties," Plaintiff cannot claim that he had a reasonable expectation of privacy for that data.

3. There Is No Serious Invasion of Privacy At Issue Here

Furthermore, the fact that the information is de-identified undermines Plaintiff's claim under *Hill*, the case cited in his pleading. As the California Supreme Court explained in that case:

> No community could function if every intrusion into the realm of private

> action, no matter how slight or trivial, gave rise to a cause of action for invasion of privacy. . . . Actionable invasions of privacy must be sufficiently serious in their nature, scope and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy. [*Hill*, 7 Cal. 4th at 37.]

Aggregating de-identified data regarding Plaintiff with other data about other pharmacy customers and their doctors cannot constitute the "egregious breach of social norms" envisioned by the California Supreme Court in *Hill*. Indeed, courts have repeatedly and resoundingly rejected privacy claims similar to plaintiff's. *See Dwyer v. American Express Co.*, 652 N.E.2d 1351, 1354-56 (Ill. Ct. App. 1995) (credit card company's compiling of lists based on customers' spending habits and selling them to marketing companies did not violate any privacy rights because there was no "unauthorized intrusion;" nor did company "appropriat[e]" plaintiffs' names or personalities); *Shibley v. Time, Inc.*, 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) ("[I]t is constitutionally permissible to sell [magazine] subscription lists to direct mail advertisers . . . [T]he practice complained of here does not constitute an invasion of privacy even if appellants' unsupported assertion that this amounts to the sale of 'personality profiles' is taken as true. . . .").

In addition, the right to information privacy must be balanced against the right to the free flow of information protected by the First Amendment. *See* First Amendment argument, *supra* at 10-12, and *Pioneer Electronics*, 40 Cal. 4th at 371 ("Assuming that a claimant has met the [three] *Hill* criteria for invasion of a privacy interest, that interest must be measured against other competing or countervailing interests in a 'balancing test'"). In this case, since the data transmissions at issue do not tell anyone that Plaintiff has ever taken any particular prescription drug, any alleged intrusion is *de minimis* and cannot counterbalance our society's need to preserve free speech.

G. The Complaint Fails to State a Cause of Action for Unjust Enrichment

A claim for unjust enrichment is equitable in nature and compels restitution if defendant is enriched *at the expense of another*. *Dinosaur Development, Inc. v. White,* 216 Cal. App. 3d 1310 (1989). "The mere fact that a person benefits another is not of itself sufficient to require the other to make restitution therefor." *Id.* For a benefit to be unjust, "it must ordinarily appear that the benefit was conferred by mistake, fraud, coercion or request." *Id.* at 1316, *quoting* 1 Witkin, Summary of Cal. Law (9th ed. 1987), Contracts, § 97 at 126.

Plaintiff alleges that Albertsons profited from its use of Plaintiff's information.[16] For this reason, Plaintiff specifically cites the CMIA as the predicate for this claim. Since the CMIA does not prohibit Defendants' use of de-identified information, there is no viable cause of action for unjust enrichment.

Furthermore, there is no apparent basis for Plaintiff to claim that he (and the class members) "own" this data, and if they do not have such a property interest, then there is no basis for a claim that Defendants profited *at Plaintiff's expense*. If Defendants were selling class members' names, addresses, or other individually identifying information, then Plaintiff might at least claim that this is information which he "owns," although the preceding discussion explains that the courts have declined to recognize such a right (see Standing argument, *supra* at 6-7). But they are not selling individually identifying information, and even Plaintiff's rather opaque Complaint does not allege that they do. Instead, as *Rowe* and *Ayotte* recognized, it is physicians who might more properly advance that claim, especially in view of the data's use to develop marketing campaigns targeted at them. Since this data is already being voluntarily transmitted to a host of third parties (see preceding fraud and privacy arguments), there is no basis to claim that one particular use of such data is "unjust" when others are permissible.

H. **California Law Does Not Recognize a Trespass Claim, Let Alone A "Trespass to Personalty" Claim**

No California case has recognized a cause of action for "trespass to personalty." The seventh cause of action appears to be a claim better known as trespass to chattel. A trespass to chattel occurs when the defendant intentionally interferes with possession of plaintiff's personal property and that interference causes the plaintiff an injury. *Thrifty-Tel, Inc. v Bezenek*, 46 Cal. App. 4th 1559, 1566-7 (1996). California has not extended the tort of interference with chattels to the use of data. This tort

---

16 Plaintiff also contends that the conduct constitutes a breach of Defendants' fiduciary duties and other duties owing to Plaintiff and members of the Class." (Compl. ¶ 74.) This legal conclusion need not be accepted as true in the absence of *facts* demonstrating how the conduct constitutes a breach of fiduciary duty or "other duties."

protects plaintiffs against "intermeddling" with their personal property, a use of that property which is not as serious as conversion. *Id.* at 1566-67. Plaintiff London *has* no personal property right in the anonymized data at issue. He therefore cannot state this claim.

Finally, since the courts have refused to recognize a property right in a plaintiff's name (see Standing argument, *supra* at 6-7), Plaintiff could not make out a trespass claim even if he could allege – which he cannot – that Defendants are selling his name to others.

I. The Complaint Fails to State a Cause of Action for a Violation of California's Unfair Competition Law

California's Unfair Competition Law ("UCL") prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Plaintiff appears to contend that the data sales at issue violate all three prohibitions.

Before turning to the reasons why Plaintiff does not and cannot allege any of the three types of UCL violations, Albertsons also refers the Court to its argument on the First Amendment (*supra* at 10-12). For the same reasons which prevent application of the CMIA to the data sales at issue, the First Amendment likewise proscribes the application of the UCL to those sales.

1. Plaintiff Cannot Allege Loss of Money or Property

Under the UCL, the only persons authorized to bring claims are those who have "suffered injury in fact and *lost money or property* as a result of [] unfair competition." Cal. Bus. & Prof. Code § 17204 (emphasis added); *Consumer Advocacy Group, Inc. v. Kintetsu Enterprises of America,* 150 Cal. App. 4th 953, 982 (2007); *Thompson v. Home Depot, Inc.*, 2007 U.S. Dist. LEXIS 68918 at *6 (S.D. Cal. September 18, 2007)(Gonzalez, C.J.). Plaintiff cannot establish the loss of either money or property. See Standing argument, *supra* at 5-7.

2. No Allegations of Unlawful Conduct

It is settled law that, in addition to identifying the statutes that constitute the predicates to a Section 17200 claim, a "plaintiff alleging unfair business practices under these statutes must state with reasonable particularity the facts supporting the statutory elements of the violation." *Khoury v. Maly's of California, Inc.*, 14 Cal. App. 4th 612, 619 (1993); *see also Accuimage Diagnostics Corp. v. Terarecon, Inc.*, 260 F. Supp. 2d 941, 955 (N.D. Cal. 2003) (requiring allegation of specific facts to state a claim under Section 17200). Here, Plaintiff fails to allege facts sufficient to state the alleged predicate violation of the CMIA for the reasons discussed above.

Plaintiff also points to other laws and regulations, none of which prohibit the alleged conduct any more than the CMIA does. Plaintiff cites the California Constitution, Article I, Section 1, which guarantees individuals the inalienable right to privacy. For the same reason that Plaintiff fails to allege a claim for invasion of privacy under *Hill*, the UCL claim cannot be based on the constitutional right to privacy. Plaintiff also cites a variety of regulations applicable to pharmacy operations. (Compl. ¶ 82(C-E).) Not surprisingly, not one of these relates to de-identified data.

3. No Allegations of Unfair Conduct

In order to prove that conduct is unfair, a plaintiff must allege that the conduct threatens a violation or offends the spirit of some law. *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 186-87 (1999); *see also Watson Laboratories, Inc. v. Rhône-Poulenc Rorer, Inc.*, 178 F. Supp. 2d 1099, 1117 (C.D. Cal. 2001). Plaintiff first attempts to satisfy this standard by alleging that Defendants' conduct constitutes violations of federal and state law. For the reasons discussed above, there are no violations of any such law.

Apart from the statutory claim, in order to properly state a claim under the "unfair" prong of the UCL, Plaintiff must allege conduct that "threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech*, 20 Cal. 4th at 187 (1999); *Watson Laboratories,* 178 F. Supp. 2d at 1117. There are no allegations of a violation of any antitrust law or comparable conduct.

4. No Allegations of Fraudulent Conduct

The case law on this element of section 17200 is still evolving, and does not provide clear guidance on the elements of a prima face claim for "fraudulent" conduct under that statute. Cases brought by plaintiffs acting in a representative capacity, seeking to remedy conduct which defrauds consumers, need not allege fraud with the specificity required in common law fraud actions. Instead, such a plaintiff states a claim for "fraudulent" conduct under section 17200 if members of the public are likely to be deceived. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992). Even under this relaxed pleading standard for fraud, Plaintiff fails to allege such deception and therefore does not state a claim for "fraudulent" unfair competition.

It is proper for a court to determine on a motion to dismiss whether a plaintiff has stated facts sufficient to show that the public is likely to be deceived by the defendant's purportedly "fraudulent" conduct. *See Haskell v. Time, Inc.*, 857 F. Supp. 1392 (E.D. Cal. 1994) (granting motion to dismiss on the ground that reasonable consumers could not be deceived by alleged false advertising); *See also Shvarts v. Budget Group, Inc.*, 81 Cal. App. 4th 1153, 1159-60 (2000) (demurrer to section 17200 "fraudulent" conduct claim properly sustained where allegations were insufficient to support the theory that the public was likely to be deceived).

As Albertsons explained in its argument for dismissal of Plaintiff's fraud claim (*supra* at 16-18), prescriber-identifiable data is routinely and properly disclosed to many third parties, and Plaintiff therefore cannot allege any likelihood that the public will be deceived by sales of data on doctors' prescribing habits. As it explained in the CMIA discussion (*supra* at 7-11), HIPAA and the CMIA both expressly permit the disclosure of de-identified medical data to third parties, which further confirms that no likelihood of deception is present here. And since the data Albertsons is selling is about doctors, not about any individual pharmacy customer, Plaintiff lacks standing to complain that these data sales mislead doctors, much less the broader "public." Most importantly, there is not and cannot be any allegation that any of the data at issue is false or misleading, so there is no basis for any claim of deception.

///

///

///

CONCLUSION

For the foregoing reasons, the Albertsons respectfully request that this Court dismiss the Complaint in this action with prejudice and grant such further relief as the Court in its discretion may deem just and proper.

Dated: July 10, 2008

DORSEY & WHITNEY LLP

By: Kathlene W Lowe

KATHLENE W. LOWE
KENT J. SCHMIDT
JOHN P. CLEVELAND
Attorneys for Defendant
NEW ALBERTSON'S, INC.